图书情报工作
第 64 卷 第 22 期 2020 年 11 月

GDPR 对科学数据开放共享个人数据保护的适用性与作用分析*

■ 盛小平　杨绍彬
上海大学图书情报档案系　上海 200444

摘　要：[目的/意义]通过分析欧盟《一般数据保护条例》(GDPR)相关规定来为我国科学数据开放共享过程中保护个人数据提供参考。[方法/过程]使用文本分析法，在述评 GDPR 与个人数据保护研究后，分析 GDPR 对科学数据开放共享个人数据保护的适用性与作用及其对我国科学数据开放共享个人数据保护的启示。[结果/结论]GDPR 对科学数据开放共享个人数据保护有许多规范作用，包括可以明确个人数据保护的基本概念与保护对象范围、主要原则、数据主体的主要权利、数据控制者与处理者的主要责任和义务，可以奠定个人数据处理的合法性基础。GDPR 给我国的启示是：我们应该建立健全我国个人数据保护法律体系，加强科学数据开放共享中个人数据的风险管理，搭建动态关联、可跟踪的科学数据开放共享系统，由此实现我国科学数据开放共享中的个人数据保护。

关键词：科学数据　开放共享　数据保护　个人数据　GDPR
分类号：G203
DOI：10.13266/j.issn.0252-3116.2020.22.005

随着大数据、互联网、云计算、物联网的发展，数据尤其是个人数据在越来越便利地被收集和传输的同时，也面临着新的威胁[1]。为了应对新技术的发展及原有保护框架的乏力，欧盟于 2018 年 5 月 25 日正式实施《一般数据保护条例》(General Data Protection Regulation，GDPR)[2]，开创了个人数据保护的欧盟模式。随后巴西和美国加州借鉴该条例分别制定了《一般数据保护法案》《加利福尼亚州消费者隐私法案》[3]。2020 年 3 月，我国更新完善后的《信息安全技术个人信息安全规范》旨在进一步遏制个人信息非法收集、滥用、泄漏等乱象，最大程度地保障个人的合法权益和社会公共利益[4]。我国的《个人信息保护法》也已进入立法阶段[5]。同时，人们已经认识到科学数据共享及再利用具有促进科学进步与创新、节约研发成本、再现科学研究等重要价值[6]。而科学数据中往往包含个人信息，尤其是在心理学、临床医学、人类学、遗传学等领域[7]。如何在科学数据开放共享的同时保护个人数据成为数据治理领域中的一个重要议题。GDPR 作为目前世界上采用最广泛的个人数据保护模式和通用规则[8]，是否适用于科学数据开放共享中的个人数据保护？到底有何作用？我国如何借鉴 GDPR 来加强科学数据开放共享中的个人数据保护？解析与回答这些问题，将有助于促进我国科学数据开放共享实践的发展。

1　相关研究述评

近几年来，国内外对 GDPR 及其个人数据保护做了大量研究。这些研究除了介绍 GDPR 的产生背景[9]、演进过程[10]、应用范围[11]、技术与组织要求[12]、关键业务[13]、结构章节与内容[14]等外，还论述了如下研究主题：①GDPR 对个人数据保护的影响。GDPR 希望用“无争议同意”与“明确同意”的区分作为保护个人数据的重要手段，即明确规定，个人数据需要获得数据主体的“无争议同意”，敏感数据则需要获得数据主体的“明确同意”[15]。在 GDPR 实施一年后，欧盟成员国家的数据保护机构一直在努力执行 GDPR 核心原则，即负责和透明地处理和保护个人数据[3]。毋庸置疑，GDPR 为其他国家进行个人数据保护立法树立了

* 本文系国家社会科学基金项目“开放科学环境下的科学数据开放共享机制与对策研究”(项目编号：18ATQ007)研究成果之一。
作者简介：盛小平(ORCID：0000-0002-6341-6973)，教授，博士，博士生导师，E-mail：@shengxp68@126.com；杨绍彬(ORCID：0000-0001-9190-8097)，硕士研究生。
收稿日期：2020-06-09　修回日期：2020-08-08　本文起止页码：48-57　本文责任编辑：徐健

一个很好的典范，具有许多积极意义，包括：GDPR 影响司法审判管辖，扩大数据保护法律域外效力，为数据跨境传输的国际共识提供规则指引，促使世界其他地区健全数据保护立法[9]18-30；GDPR 扩张了个人数据保护适用范围，扩大了数据主体的权利，加重了数据控制者和处理者的义务，强化了个人数据的监管和救济机制[16]；GDPR 弥补了一些法律漏洞，个人因而能够更好地控制自己的个人数据，同时对于企业之间良好竞争环境的营造也大有裨益；GDPR 既保证了成员国监管机构之间更高效的合作，又使得企业与监管机构的沟通更为方便，个人在数据面临侵害时也有了有效的维权方式。但是，GDPR 还存在着问题与争议，包括：其某些制度（如知情同意制度等）存在缺陷、某些问题界定不明晰、GDPR 的执行效果还存在疑问、存在如何平衡个人数据保护与其他法益之间的问题[16]。②GDPR 实施个人数据保护的重点领域或主题。GDPR 涉及个人数据保护的方方面面，但重点是强化数据主体对于数据的控制权，即数据的人格权与财产权保护[14]；倡导建立数据保护官制度来实施个人数据的保护[17]；规范了跨境流动数据保护[18]、数据可携带权[19]、数据被遗忘权[20-21]等核心问题。③GDPR 在不同领域个人数据保护的应用研究。这包括患者隐私保护[22]、跨境数据流通与保护[23]、数据保护影响评估[24-25]、科研数据出版中的数据保护问题[26]、智慧图书馆用户数据隐私保护[27]、物联网对数据控制者和加工者的数据保护[28]等。④GDPR 对我国个人数据保护的启示。主要包括：我国应借鉴欧盟《通用数据保护条例》立法理念，从法律、社会治理以及信息产业等维度构建个人信息双轨保护制度[29]；我国应该借鉴效果原则的立法思路，确立场景化和技术化的数据保护理念，合理地引入“撤销同意”模式，发挥事前监管和救济的作用[16]；我国立法应构建信息主体、其他自然人、国家机关、企业四方主体共享的个人信息权益体系，以妥善解决各方主体之间的权益冲突[30]；我国应该构建基于 GDPR 的个人数据保护企业自评指标体系[31]；我们应该认识到，尽管 GDPR 规范了欧盟个人数据保护，但欧盟与中国分享个人数据具有挑战性，目前仅能分享匿名数据或获得数据主体同意的数据[32]。总之，GDPR 是个人数据保护的一种法律框架，规定了在其适用范围内处理个人数据时必须采用的关键原则和保障措施，对我国实施个人数据保护有重要的参考价值。不过，目前鲜见 GDPR 在科学数据开放共享个人数据保护中的相关研究，尽管人们发现，GDPR 在处理遗传数据共享[33]、临床医学研究[34]等方面都产生了广泛影响。

2 GDPR 对科学数据开放共享个人数据保护的适用性分析

科学数据开放共享旨在促使科学数据不受限制地被获取和再利用，以实现科学数据价值最大化和促进开放研究与开放创新。它将科学数据置于开放环境，要求个人或机构在开放科学数据时必须按照相应的规范和采取适当的措施来实施数据保护。数据保护是指实施适当的行政、技术或物理措施，将未经授权或意外造成的数据泄露的风险或损害最小化[35]。个人数据保护旨在保护公民的权利、个人数据完整性和个人隐私[36]，不仅涉及相关的法律、法规、政策，还涉及收集、存储、处理数据的技术与系统等[37]。GDPR 是否适用于科学数据开放共享个人数据保护？要回答此问题，需要了解 GDPR 的结构与内容。

2.1 GDPR 结构与内容

GDPR 是一部庞大、复杂的数据保护法，在结构上分法释（recitals，共 173 条）和正文（共 11 章、99 条）两部分，共 88 页，约 55 000 字。GDPR 可为保护欧洲人的个人数据以及促进一系列合法目的负责任的数据处理提供一个全面的法律框架。它彻底整治了组织收集、使用和共享个人数据的方式[38]。正文包括如下 11 章内容[2]：①一般条款，明确了 GDPR 所涉及的主要事项与目标、适用范围、地域管辖范围以及相关概念的定义；②原则，明确了个人数据保护的 7 项原则——“合法性、合理性和透明性”原则、“目的限制”原则、“数据最小化”原则、“准确性”原则、“存储限制”原则、“完整性与保密性”原则、“责任性”原则；③数据主体的权利，规定了数据主体拥有的 7 项权利；④控制者和处理者，规定了数据控制者和处理者的责任；⑤将个人数据转移到第三国或国际组织，规定了将个人数据转移到第三国或国际组织的要求；⑥独立监管机构，规定了监管机构的独立性地位、一般要求、职权、任务与权力等；⑦合作与融贯性，规定了领导性监管机构和其他相关监管机构的合作、协助与联合行动以及一致性解决办法；⑧救济、责任与惩罚，规定了数据主体向监管机构进行申诉的权利，针对监管机构、控制者或处理者的有效司法救济权，获取赔偿的权利与责任，行政罚款的一般条件等；⑨与特定处理情形相关的条款，规定了处理、表达自由与信息，为了实现公共利益、科学或历史

研究或统计目的处理中的安全保障和减损等；⑩授权法案与实施性法案，规定了对授权的行使、委员会程序；⑪最后条款，明确了95/46/EC指令的废止、和之前已经达成的协议的关系、委员会的报告义务、生效与适用等内容。

2.2 GDPR对科学数据开放共享个人数据保护的适用性解析

GDPR涉及个人数据保护的方方面面，强化了数据主体对于数据的控制权，明确个人数据保护的一些概念、原则、权利、责任、监管要求，同样适用于科学数据开放共享中的个人数据保护。这主要体现在如下4个方面：

（1）科学数据开放共享中的个人数据属于GDPR界定的保护对象范畴。GDPR第2条"适用范围"第1款规定："本条例适用于全部或部分以自动方式的个人数据处理，以及除自动方式外的其他方式的个人数据处理，这些个人数据构成存档系统的一部分或旨在构成存档系统的一部分。"[2]这里，"个人数据"是指与已识别或可识别的自然人（"数据主体"）相关的任何信息；一个可识别的自然人是一个能够被直接或间接识别的个体，特别是通过姓名、身份编号、位置数据、在线标识符或者自然人所特有的一项或多项的物理、生理、遗传、心理、经济、文化或社会性身份[2]。根据GDPR对个人数据的定义，可以发现，个人数据既包括可直接识别出数据主体的信息（如姓名），又包括通过结合其他信息而间接识别数据主体的信息（如电话号码、护照号码、生物特征等）[39]。科学数据开放共享中的个人数据属于GDPR界定的个人数据范畴，通常以实验、测量、现场观察、调查结果、采访记录和图像等形式出现[40]，所以GDPR可以用来规范与保护开放共享中的个人数据。

（2）科学数据开放共享是一种特殊的数据"处理"活动，可以纳入GDPR界定的"处理"活动范畴，因而能够受到GDPR的保护。GDPR第4条"定义"第2款规定："'处理'是指任何一项或多项针对单一个人数据或系列个人数据所进行的操作行为，不论该操作行为是否采取自动化方式，如收集、记录、组织、构造、存储、调整或更改、检索、咨询、使用、通过传输而公开、传播或以其他方式利用、排列或组合、限制、删除或销毁。"[2]科学数据开放共享是一类特殊的数据处理活动。因为在科学数据开放共享中，无论是科研人员进行的数据收集、记录、存储、汇交、上传等行为，还是使用者访问、获取、传输、再利用等行为均构成对个人数据的处理。换言之，个人数据的处理贯穿整个科学数据开放共享价值链的全过程。因此，GDPR适用于科学数据开放共享中的个人数据保护。

（3）GDPR的"地域范围"已经超过了欧盟成员国的地理边界，适用于开放共享环境。GDPR第3条"地域范围"规定[2]："①本例适用于在欧盟内部设立的数据控制者或处理者对个人数据的处理，不论其实际数据处理行为是否在欧盟内进行。②本条例适用于如下相关活动中的个人数据处理，即使数据控制者或处理者不在欧盟设立：（a）为欧盟内的数据主体提供商品或服务——不论此项商品或服务是否要求数据主体支付对价；或（b）对发生在欧洲范围内的数据主体的活动进行监控。③本条例适用于在欧盟之外设立，但基于国际公法成员国的法律对其有管辖权的数据控制者的个人数据处理。"上述3个条款特别是第3款，实质上把开放共享的个人数据纳入保护范围，不管该数据控制者是否在欧盟之内。

（4）GDPR能够为科学研究提供个人数据保护，实质上也能为科学数据开放共享提供个人数据保护。GDPR不包含科学研究的正式定义，从广义的研究概念出发，指出"应以广泛的方式，包括诸如技术开发和展示、基础研究、应用研究和私人资助研究，来解释为科学研究目的的个人数据的处理"[41]。GDPR在法释的第26条、第33条等14处以及正文中第5条、第89条等6处，都提到与"研究"相关的规制。例如，第156条法释规定[2]："为了公共利益的存档目的、科学或历史研究目的或统计目的而处理个人数据，应根据本条例，对数据主体的权利和自由给予适当保障。欧盟成员国应为为了公共利益的存档目的、科学或历史研究目的或统计目的而处理个人数据提供适当保障。"这意味着，为科学或历史研究目的处理个人数据时应保障数据主体的权利和自由，欧盟成员国应为此提供适当保障。又如，正文第89条第1款规定[2]："为了公共利益的存档目的、科学或历史研究目的或统计目的的进行的数据处理，应当为数据主体的权利与自由采取符合本条例的适当保障措施。应当采取技术与组织性措施以确保遵守数据最小化原则。这些措施可以包括化名。"正文第89条第2款规定[2]："在为科学或历史研究目的或统计目的处理个人数据时，欧盟或成员国的法律可以按照第89条第1款所规定的情形与保障措施对第15、16、18、21条所规定的权利进行克减，如果此类

权利可能彻底阻碍或严重阻碍实现上述特殊目的，且此类克减对于实现这些目的是必要的。”这两项条款实质上不仅要求为科学或历史研究目的进行的数据处理提供适当保障措施，而且可以获得数据主体访问权、修正权、限制处理权、反对权的克减，从而更利于这些个人数据的共享与利用。由于科学研究从广义上包含科学数据开放共享活动，科学数据开放共享可以更好地促进科学研究，所以，GDPR 为科学或历史研究目的制定的相关个人数据保护条款也适用于科学数据的开放共享活动。

3 GDPR 对科学数据开放共享个人数据保护的作用分析

作为一部欧盟成员国法律，GDPR 既可直接适用于欧盟范围内的所有企业与公民，又具有较强的域外效力，无论数据处理行为是否发生在欧盟境内，只要数据涉及欧盟内的数据主体就要受到 GDPR 的规制。GDPR 从适用范围、数据保护原则、数据主体权利、数据控制者与处理者的责任与义务、跨境数据传输机制、数据监管机构、行政处罚等方面构建了完整的个人数据保护框架。对于科学数据开放共享个人数据保护而言，GDPR 的作用主要体现在如下几方面：

3.1 可以明确个人数据保护的基本概念与保护对象范围

GDPR 第 4 条“定义”界定了 26 个核心概念，包括个人数据、处理、限制处理、用户分析(profiling)、假名化(pseudonymisation)、归档系统(filing system)、控制者、处理者、接收者、第三方、同意、个人数据泄露、遗传数据、生物性识别数据、和健康相关的数据、主要机构(main establishment)、代表、企业、企业集团(group of undertakings)、有约束力的公司规则、监管机构、相关监管机构、跨境处理、相关和合理的异议、信息社会服务、国际组织。这些术语的界定为科学数据开放共享个人数据保护确立了一些核心概念与基本理念。例如，把 GDPR 定义的“个人数据”概念运用到科学数据开放共享中，这时个人数据保护不仅仅是个人财产权数据或人格权数据的保护，更不是狭义的个人隐私数据的保护，而是广义的“与已识别或可识别的自然人(“数据主体”)相关的任何信息”的保护。“个人数据”定义明确，可以帮助人们理解科学数据开放共享中的个人数据保护到底需要保护哪些与个人相关的数据。

作为一部个人数据保护法，GDPR 区分了 4 种不同类型的个人数据——个人数据、特殊类型的个人数据、假名化数据和匿名数据。在 GDPR 中，个人数据概念具有广泛的范围。特殊类型的个人数据，也称为“敏感个人数据”，包括：①显示种族或族裔出身的数据；②政治见解；③宗教或哲学信仰；④工会会员资格；⑤遗传数据；⑥生物性识别数据；⑦有关健康的数据；⑧关于性生活或性取向的数据。这些敏感个人数据对数据主体具有更高程度的风险，一般是禁止处理的，只有在处理必须有合法的依据且处理符合 GDPR 第 9 条第 2 款所列的 10 种特殊条件之一下才被允许处理[38]。个人数据的假名化是指以不使用其他信息就不能使个人数据再归于某一特定数据主体的方式对个人数据的处理，只要这些其他信息被分开保存且采取技术和组织措施以确保个人数据不归于已识别或可识别的自然人[2]。假名化个人数据仍然属于 GDPR 定义的个人数据范围，它被视为在技术和组织措施概念下的一种安全保障，但这些技术不能用来规避依据 GDPR 的遵守合规义务[41]。GDPR 没有对匿名数据进行定义，但在其法释的第 26 条明确规定：“数据保护原则不应适用于匿名信息，即与已识别或可识别的自然人无关的信息，或以不能识别或不再识别数据主体的方式匿名的个人数据。因此，本条例不涉及处理此类匿名信息，包括用于统计或研究目的。”[2] 由此看来，GDPR 适用于假名化数据，而不适用于匿名数据。这就意味着，科学数据开放共享中的假名化数据应该按照 GDPR 来进行处理，而处理匿名数据不会触发个人数据保护法[42]。这种区分对于实施科学数据开放共享个人数据保护具有很大的指导意义。

3.2 可以明确个人数据保护的主要原则

GDPR 第 5 条定义了如下个人数据处理原则[2]：①合法性、合理性和透明性(对涉及到数据主体的个人数据，应当以合法的、合理的和透明的方式来进行处理。②目的限制(为特定、明确和合法的目的收集，而不是以不符合这些目的的方式进一步处理个人数据；为了公共利益的存档目的、科学或历史研究目的或统计目的而进行的进一步处理，不视为违反初始目的)。③数据最小化(个人数据处理应当是充分的、相关的，并限于与处理它们的目的相关的必要内容)。④准确性(个人数据应当是准确的，并在必要时保持最新；考虑到处理这些数据的目的，必须采取一切合理手段，确保不准确的个人数据立即被擦除或纠正)。⑤存储限制(对于能够识别数据主体的个人数据，其储存时间不

得超过为处理个人数据的目的所必需的时间；个人数据可保存较长的时间，只要个人数据的处理完全是为了公共利益的存档目的、科学或历史研究目的或统计目的且执行了本条例要求的适当技术和组织措施来保障数据主体的权利和自由）。⑥完整性与保密性（处理过程中应确保个人数据的安全，采取合理的技术和组织措施，避免数据未经授权即被处理或遭到非法处理，避免数据发生意外毁损或灭失）。以确保个人数据适当安全的方式处理个人数据，包括使用适当的技术或组织措施，防止未经授权或非法处理，防止意外损失、销毁或损坏）。⑦责任性（数据控制者应负责并能够证明遵守上述原则）。上述7个原则同样是科学数据开放共享个人数据保护必须遵循的主要原则，因为根据GDPR对处理的广义定义，为科学目的转移个人数据（包括科学数据开放共享）被视为一种处理形式，因此应符合GDPR的实质性规范[32]。换句话说，GDPR确立了科学数据开放共享个人数据保护应遵循的主要原则。

3.3 可以奠定个人数据处理的合法性基础

存在数据处理的合法性基础既是个人数据处理的重要前提，也是个人数据保护的重要保障。GDPR第6条第1款规定了6项数据处理的合法性基础，包括数据主体的同意、履行合同的需要、履行法律义务的需要、保护数据主体或另一个自然人的核心利益的需要、为了公共利益或基于官方权威而履行某项任务的需要、追求合法利益的需要。GDPR第6条第2至4款更加细致地规范了第1款数据处理需满足的条件。这些合法性基础同样为科学数据开放共享中的个人数据处理提供了合法、合理的依据。

第一，对于科学数据开放共享而言，取得数据主体的同意是合法处理个人数据最稳妥、最基本的方式。在GDPR中，数据主体的“同意”是指数据主体通过声明或明确的肯定行动，做出任何自愿、具体、知情和明确的同意处理与其有关的个人数据的意愿表示[2]。这一定义说明有效获取数据主体的同意必须同时满足“自愿”“具体”“知情”及“明确”等条件，也就是说，数据主体的“同意”并非“广泛同意”。GDPR第6条（1）款（a）项规定，如果“数据主体已同意为一项或多项具体目的处理其个人数据”，则可合法处理个人数据；而GDPR第9条（2）款（a）项规定，如果“数据主体已明确同意为一项或多项具体目的处理这些个人数据”，则可合法处理特殊类别的个人数据。换句话说，GDPR要求针对一般个人数据的处理需征得数据主体的“无争议同意”，而针对敏感个人数据的处理需征得数据主体的“明确同意”[15]。2019年，谷歌因违反GDPR而被法国国家信息与自由委员会处以5 000万欧元罚款，做出处罚的主要原因是谷歌违反了控制者的信息披露义务和谷歌未有效取得用户同意[43]。

第二，除数据主体的“无争议同意”和“明确同意”是个人数据处理的合法性基础以外，公共利益和合法利益也是在科学数据开放共享过程中处理个人数据的法律依据。不过，（非私营）大学和公共研究机构等公共当局在执行公共任务时，不能以“合法利益”为依据而须在法律授权的情况下或依靠“符合公共利益的任务或行使赋予控制者的官方权力”作为其法律依据，进行个人数据处理[38]。

第三，GDPR为与科学数据开放共享紧密关联的二次数据使用和跨境数据转移提供了法律依据。通常，严格的“目的限制”原则适用于“不能以不符合最初收集和处理个人资料的具体和合法目的的方式被进一步处理的个人数据”。然而，GDPR第5条（1）款（b）项规定，为科学研究目的而做的进一步处理，依据GDPR第89条（1）款，不得视为与最初的数据处理目的不相容。这意味着，如果同一组织或另一组织正在对数据进行进一步处理（即二次使用），则有一种可反驳的推定，即为科学研究目的进行的进一步处理与最初说明的处理目的（例如，为了医疗诊断）是一致的。在适用的成员国法律允许的情况下，根据第89条（2）款，科学研究例外允许的对数据主体权利的豁免将适用于这种情况。这实质上为二次数据使用及其开放共享奠定了法律基础。

第四，科学数据开放共享涉及国际（或跨境）数据转移问题，这时可参考GDPR对国际数据转移的规定。依据GDPR，在欧盟以外合法转移个人数据有5种途径：①基于适足性决定的转移（GDPR第45条）；②有适当保障措施的转移（GDPR第46条）；③基于有约束力的公司规定的转移（GDPR第47条）；④未经联盟法律授权的转移或披露（GDPR第48条）；⑤基于特殊情形下豁免的转移（GDPR第49条）。由于开放共享本身包含数据跨境转移或国际转移，依据GDPR，数据控制者必须在向数据主体收集个人数据时告知数据主体，控制者打算将这些个人数据实施开放发布，并决定采取哪种合适的途径。在没有适足性决定情况下，如果数据控制者或处理者有适当的保障措施和可强制执

行的数据主体权利,并且有有效的法律补救办法,数据仍然可以开放发布或转移到第三国或国际组织[38]。

第五,GDPR 第 89 条为实现公共利益、科学或历史研究或统计目的的个人数据处理,提供了专门的“安全保障与免责”规定——在采取保证数据最小化原则的技术与组织措施(如匿名化)、保障数据主体的权利与自由的前提下,当数据主体的访问权、修正权、限制处理权、反对权可能彻底阻碍或严重阻碍实现公共利益、科学或历史研究或统计目的的数据处理时,可以豁免上述数据主体的权利,但仅当这种豁免是实现上述目的的必不可少时[2]。也就是说,在为科学研究目的处理个人数据时,存在一些例外,比如,并不总是需要数据主体的同意,而是其他合法性基础,如合同、遵守法律义务、公共利益或控制者或第三方追求的合法利益;个人数据的保存时间可以超过处理所需的时间等[44]。

总之,GDPR 通过提供 6 项数据处理的合法性基础,特别是对“同意”、二次数据使用、跨境数据转移、科研研究的例外(豁免)的明确,可以为科学数据开放共享中的个人数据保护提供广泛的法律依据。

3.4 可以明确数据主体的主要权利

数据主体是指其个人数据正在被收集,保存或处理的任何人[45]。GDPR 赋予数据主体如下 8 项基本的数据权利[2]:①知情权:是指数据控制者在收集与数据主体相关的个人数据时,应当告知数据主体,包括数据控制者的身份与详细联系方式、数据处理将涉及的个人数据的使用目的,以及处理个人数据的法律依据等;②访问权:是指数据主体有权从数据控制者那里得知关于其个人数据是否正在被处理的真实情形,如果其数据正在被处理的话,数据主体应当有权访问个人数据并有权获知相关信息;③修正权:是指数据主体有权要求数据控制者及时地纠正与其相关的不准确个人数据;④撤回同意权:是指数据主体有撤回先前为某种目的处理其个人数据而给予的同意并要求数据处理者停止根据先前提供的同意处理个人数据的权利;⑤限制处理权:是指在特定情况下,数据主体有权限制数据控制者处理数据;⑥反对权:是指数据主体基于合法或合理的原因反对数据控制者对其个人数据进行处理的权力,比如反对因直接营销目的而处理个人数据、反对非执行公共利益的某项任务必不可少的科学或历史研究目的或统计目的而进行的个人数据处理;⑦删除权(被遗忘权):是指数据主体有权要求数据控制者及时删除或擦除其个人相关数据的权利;⑧可携带权:是指数据主体有权以结构化、通用和机器可读的格式接收其提供给数据控制者的相关个人数据,并有权将这些数据不受已提供个人数据的控制者的阻碍,传输给另一个数据控制者。

在科学数据开放共享活动中,数据主体同样拥有上述权利,也就是说,必须尊重与保护上述数据主体权利来实施科学数据开放共享中的个人数据保护。例如,数据可携带权旨在平衡数据流动的自由和管制,使数据主体能以简明方式迁移数据并更好地控制个人数据。它由两项相互独立的请求权构成,即数据主体获得个人数据的权利、要求数据控制者和处理者向其他主体提供个人数据的权利。前者是获取个人数据副本的权利,后者是将个人数据从某一控制者直接传输到另一控制者的权利[10]。落实数据主体的这一权利是实施科学数据开放共享的关键。反之,若否定数据可携带权,科学数据开放共享就会面临许多困境与障碍。

3.5 可以明确数据控制者与处理者的主要责任和义务

GDPR 不仅明确了数据主体的主要权利,而且界定了数据控制者与处理者的主要义务。在 GDPR 中,数据“控制者”是指单独或与他人共同决定处理个人数据的目的和方法的自然人或法人、公共机构、其他机构或团体;如果这种处理的目的和手段是由欧盟或成员国法律确定的,那么对控制者的定义或确定控制者的标准应当由欧盟或成员国的法律来规定;数据“处理者”是指代表数据控制者处理个人数据的自然人或法人、公共机构、其他机构或团体[2]。

依据 GDPR 规定,数据控制者与处理者需要承担一些共同的义务,包括:①控制者和处理者应当配合监管机构的工作(GDPR 第 31 条);②控制者和处理者应当采取适当的技术与组织措施以保证与风险相称的安全水平(GDPR 第 32 条 1 款);③在公共机构处理操作或处理需要大规模地对数据主体进行常规和系统性的监控,或处理包含对某种特殊类型数据的大规模处理和对定罪和违法相关的个人数据的处理时,控制者和处理者应当委任数据保护官(GDPR 第 37 条 1 款);④控制者和处理者应当支持数据保护官履行其责任,并提供必要资源(GDPR 第 38 条 2 款)。

除此之外,数据控制者还要履行如下义务:①控制者应当对数据主体行使其权利提供帮助(GDPR 第 12 条 2 款);②当收集与数据主体相关的个人数据时,控制者应当为数据主体提供相关信息,如控制者的身份与详细联系方式、数据保护官的详细联系方式、处理将

要涉及到的个人数据的目的、个人数据的接收者等(GDPR 第 13 条 1 款);③除特殊情况以外,控制者有责任应数据主体的合理要求及时擦除个人数据(GDPR 第 17 条 1 款);④控制者应当采取适当的技术与组织措施,保证处理符合 GDPR 规定(GDPR 第 24 条 1 款);⑤控制者需采取适当的技术与组织措施,以保障在默认情况下只有某个特定处理目的所必要的个人数据被处理(GDPR 第 25 条 2 款);⑥每个控制者都应当保持其所负责的处理活动的记录(GDPR 第 30 条 1 款);⑦控制者在知悉个人数据泄露后应当及时(最迟在 72 小时内)将个人数据泄露告知相关主管监管机构(GDPR 第 33 条 1 款);⑧当个人数据泄露很可能给自然人的权利与自由带来高风险时,控制者应当及时向数据主体传达个人数据泄露(GDPR 第 34 条 1 款);⑨当某种类型的处理很可能会对自然人的权利与自由带来高风险时,控制者应当在处理之前评估计划的处理进程对个人数据保护的影响(GDPR 第 35 条 1 款);⑩当数据保护影响评估表明,如果控制者不采取措施,处理会带来高风险时,控制者应当在处理之前咨询监管机构(GDPR 第 36 条 1 款)。

另外,数据处理者还要履行的义务包括:①每个处理者对于以控制者名义进行的处理都应当保持保存一份记录(GDPR 第 30 条 2 款);②处理者在获知个人数据泄露后,应当及时告知控制者(GDPR 第 33 条 2 款)。

总之,数据控制者和处理者有义务遵守 GDPR 的各项原则及规定,包括需要承担保障数据主体权利、采取技术和组织措施、处理记录保存、数据泄漏通知、数据保护影响评估等多种义务。由于在科学数据开放共享中,科学数据生产者(如研究人员、研究机构、图书情报机构、数据中心、出版社、其他企业、政府等)、组织者(如图书情报机构、数据中心、政府等)、发布者或出版者(如研究人员、研究机构、图书情报机构、行业协会、出版社、其他企业、政府等)、传播者(如图书情报机构、数据中心、行业协会、出版社、其他企业、政府等)、管理者(如图书情报机构、数据中心、出版社、其他企业、政府等)[46],都可能成为数据控制者或处理者,所以 GDPR 有助于明确利益相关者在科学数据开放共享个人数据保护中的责任和义务,并提供法律保障。

4 GDPR 对我国科学数据开放共享个人数据保护的启示

综上所述,GDPR 主要从适用范围、数据保护原则、数据处理的合法性基础、数据主体的权利、控制者及处理者的义务等方面在整个欧盟建立起统一的数据保护法律框架,不仅为欧盟内外的个人数据保护提供了法律保障,而且较好地维持了个人数据保护与科学数据开放共享之间的平衡。它可以为我国科学数据开放共享个人数据保护提供如下借鉴与启示:

4.1 建立健全我国个人数据保护法律体系

为有效实施我国科学数据开放共享中的个人数据保护,关键在于建立健全我国个人数据保护法律体系。目前,我国尚未制定专门的个人数据保护法,与个人数据保护的法律法规及相关文件主要有:《信息安全技术公共及商用服务信息系统个人信息保护指南》《刑法修正案(九)》《侵权责任法》《消费者权益保护法》《关于加强网络信息保护的决定》《规范互联网信息服务市场秩序若干规定》《电信和互联网用户个人信息保护规定》《网络安全法》《民法总则》《信息安全技术个人信息安全规范》《科学数据管理办法》以及将于 2021 年 1 月 1 日开始实施的《民法典》等。虽然最新的《民法典》制定了"自然人的个人信息受法律保护"条款,要求"处理个人信息,应当遵循合法、正当、必要原则,不得过度处理,并符合下列条件:①征得该自然人或其监护人同意,但法律、行政法规另有规定的除外;②公开处理信息的规则;③明示处理信息的目的、方式和范围;④不违反法律、行政法规的规定和双方的约定"[47]。但是,对照 GDPR,我国现有规定存在如下不足[48-49]:①不同法律文本对相同或相似内容的用语和规定不统一、边界不清,存在交叉重复,不利于权利义务设置的互相衔接和行使中协调一致。②规制的义务主体不全面,未特别强调容易泄露的行为主体。③义务条目与内容过于原则,不够具体、明确和凝练;关于泄露的规定针对性不强、细化不足。④隐私权与数据保护权之间没有正式区别开来。⑤没有为个人提供正式和可利用的司法补救办法。因此,我国应该建立健全我国个人数据保护法律体系,包括:①尽快出台《个人信息保护法》《数据安全法》,不仅全面保护个人数据的存储和使用,而且还将为个人提供访问权、修正权和被遗忘的数据主体权利,并引入责任模式[38],从适用范围、数据保护原则、数据处理的合法性基础、数据主体权利、控制者及处理者的义务等方面确立个人数据保护的法律框架。②制定专门的科学数据管理与开放共享办法,明确数据主体对其个人数据所拥有的数据权利,如知情权、访问权、修正权、删除权、限制处理

权、数据可携带权、反对权等,详细规范个人数据的处理与开放共享行为。2019 年 2 月 11 日,中国科学院(以下简称"中科院")率先在国内制定了系统内的规范性文件——《中国科学院科学数据管理与开放共享办法(试行)》。该办法明确了科学数据开放共享主体责任、科研项目数据汇交要求,建立了论文关联数据汇交机制,规划了中科院科学数据中心[24],但未规范与个人数据保护相关的数据权利,很难有效指导与实施科学数据开放共享中的个人数据保护。正因为如此,今后国内其他机构应该把个人数据保护纳入本单位科学数据管理与开放共享办法中,以便实现促进科学数据的开放共享和有效保护个人数据的双重目的。

4.2 加强科学数据开放共享中个人数据的风险管理

GDPR 以风险为导向,将个人数据保护的义务和责任转移到数据控制者与处理者身上,为数据控制者和处理者设定了多项义务,包括执行数据泄露通知和数据保护影响评估、设置数据保护官制度等,不仅可以主动预见风险、识别风险与应对风险,而且可以更好地保障数据主体权利[50]。因此,在我国科学数据开放共享个人数据保护过程中,特别是当数据处理方式可能给自然人权利和自由造成高风险时,数据控制者应当对预期的处理操作进行个人数据保护影响评估。这种评估可按照数据处理、高风险识别、咨询数据保护官或数据主体、制作数据处理操作清单、事后复审的流程来进行[51]。不过,数据保护影响评估过程不是一次性活动,而是在处理条件和情况发生变化时,特别是在数据主体权利和自由面临风险的情况下,数据控制者需要执行的持续活动[50]。这时,开展科学数据开放共享的机构(如政府部门、研究机构、图书情报机构、数据中心、出版社、其他企业等)需要设置与任命数据保护官,以便监管数据控制者或处理者对于个人数据保护政策的遵守情况、参与数据保护影响评估、提供咨询与建议等,从而为个人数据保护提供安全保障。

4.3 搭建动态关联、可跟踪的科学数据开放共享系统

GDPR 赋予了数据主体极为系统且完整的数据权利,要求数据控制者必须采取积极的措施以尽可能地保障权利。然而,由于数据控制者与处理者的风险管理能力与认知能力存在差异,因此很难达到一致且高水平的数据保护状态。又因为数据控制者与接收者的使用目的与方式往往不同,GDPR 无法解决科学数据开放共享后的个人数据失控问题。例如,数据主体行使删除权时,控制者虽然会采取一定措施通知数据接收者,但其无法保证删除权的真正实现。目前我国的科学数据开放共享基础设施还不健全,难以将科学数据开放共享中的个人数据保护保持在较高的水平,应考虑搭建动态关联、可跟踪的科学数据开放共享系统,包括专用的开放关联的科学数据共享平台、动态的科学数据开放共享登记系统、禁止数据接收者进行数据再识别和追踪数据使用者的机制,从而实现科学数据开放共享与个人数据保护的完美结合。

参考文献:

[1] LAMBERT P. Understanding the new European data protection rules[M]. Boca Raton: CRC Press, 2018:35.

[2] THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[EB/OL]. [2020 - 08 - 04]. https://eur-lex. europa. eu/legal-content/EN/TXT/PDF/? uri = CELEX:32016R0679.

[3] BREITBARTH P. The impact of GDPR one year on[J]. Network security,2019 (7):11 - 13.

[4] 中国电子技术标准化研究院.《信息安全技术 个人信息安全规范》(2020 年版)国家标准正式发布[EB/OL]. [2020 - 08 - 06]. http://www. cesi. cn/202003/6213. html.

[5] 王比学. 个人信息保护法已列入立法规划[N]. 人民日报,2019 - 06 - 05(4).

[6] PASQUETTO I V, RANDLES B M, BORGMAN C L. On the reuse of scientific data[J]. Data science journal,2017,16(8):1 - 9.

[7] PAUL Q, LIAM Q. Big genetic data and its big data protection challenges[J]. Computer law & security review, 2018,34(5):1000 - 1018.

[8] SULLIVAN C. EU GDPR or APEC CBPR? a comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era[J]. Computer law & security review, 2019,35(4):380 - 397.

[9] 李明阳. 论欧盟通用数据保护制度与中国的法律应对——以《通用数据保护条例》为切入点[D]. 上海:华东政法大学,2019:12 - 14.

[10] 金晶. 欧盟《一般数据保护条例》:演进、要点与疑义[J]. 欧洲研究,2018, 36(4):1 - 26.

[11] 欧洲数据保护委员会,敖海静. 关于《一般数据保护条例》适用的地域范围的指南[J]. 经贸法律评论,2020(2):135 - 158.

[12] SHARMA S. Data privacy and GDPR handbook[M]. Hoboken: John Wiley & Sons, Inc. ,2020.

[13] ZIEGLER S, EVEQUOZ E, HUAMANI A M P. The impact of the European General Data Protection Regulation (GDPR) on future data business models: toward a new paradigm and business opportunities[M]//AAGAARD A. Digital business models: driving transformation and innovation. Cham: Springer Nature Switzerland AG,2019:201 -226.
[14] 丁晓东. 什么是数据权利? ——从欧洲《一般数据保护条例》看数据隐私的保护[J]. 华东政法大学学报,2018(4):39 -53.
[15] 王雪乔. 论欧盟 GDPR 中个人数据保护与"同意"细分[J]. 政法论丛,2019(4):136 -146.
[16] 吴琳玲. 欧盟 2016 年《一般数据保护条例》研究[D]. 武汉:武汉大学,2017.
[17] 刘江山. 欧盟通用数据保护条例中的数据保护官制度[J]. 中国科技论坛,2019(12):173 -179.
[18] 杨雪. 欧盟法中的个人数据保护问题研究——以欧盟跨境流动数据的保护为核心[D]. 北京:外交学院,2017.
[19] 沈煜昊. 欧盟《一般数据保护条例》中的数据可携权研究[D]. 上海:上海外国语大学,2019.
[20] POLITOU E, MICHOTA A, ALEPIS E, et al. Backups and the right to be forgotten in the GDPR: An uneasy relationship[J]. Computer law & security review,2018,34(6):1247 -1257.
[21] 卢冰洋. 欧盟《通用数据保护条例》中被遗忘权制度研究[D]. 上海:上海师范大学,2020.
[22] 耿希,顾翠峰,马俊坚. 欧盟《一般数据保护条例》对我国患者隐私保护的启示[J]. 中国医学伦理学,2019,32(8):1000 -1003,1009.
[23] MULDER T,TUDORICA M. Privacy policies, cross-border health data and the GDPR[J]. Information & communications technology law, 2019,28(3):261 -274.
[24] BIEKER F, MARTIN N, FRIEDEWALD M, et al. Data protection impact assessment: a hands-on tour of the GDPR's most practical tool[C]//HANSEN M, KOSTA E, NAI-FOVINO I, et al. Privacy and identity management: the smart revolution. Cham: Springer International Publishing AG, 2018:207 -220.
[25] CORTINA S, VALOGGIA P, BARAFORT B. Designing a data protection process assessment model based on the GDPR[C]//WALKER A, O'CONNOR R V, MESSNARZ R. Systems, software and services process improvement. Cham: Springer Nature Switzerland AG, 2019: 136 -148.
[26] 许鑫,毛璐. 科研数据出版中的数据保护问题研究——基于欧盟 GDPR 的启示[J]. 信息资源管理学报,2010,10(2):99 -106.
[27] 陆康,刘慧,任贝贝,等. 智慧图书馆用户数据隐私保护研究——基于《中华人民共和国网络安全法》和《一般数据保护条例》的文本启示[J]. 图书馆理论与实践,2020(3):17 -21.
[28] LOIDEAIN N N. A port in the data-sharing storm: the GDPR and the Internet of things[J]. Journal of cyber policy, 2019,4(2):178 -196.
[29] 林凌,李昭熠. 个人信息保护双轨机制:欧盟《通用数据保护条例》的立法启示[J]. 新闻大学,2019(12):1 -15,118.
[30] 商希雪. 超越私权属性的个人信息共享——基于《欧盟一般数据保护条例》正当利益条款的分析[J]. 法商研究,2020,37(2):57 -70.
[31] 许济沧,安小米,孙嘉睿,等. 基于 GDPR 的个人数据保护企业自评指标体系研究[J]. 图书情报工作,2018,62(23):113 -118.
[32] DEURSEN S, KUMMELING H. The new silk road: a bumpy ride for Sino-European collaborative research under the GDPR? [J]. Higher education, 2019,78(5):911 -930.
[33] SHABANI M, BORRY P. Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation[J]. European journal of human genetics, 2018, 26(2):149 -156.
[34] DEMOTES-MAINARD J, CORNU C, GUERIN A, et al. How the new European data protection regulation affects clinical research and recommendations? [J]. Therapie,2019, 74(1):31 -42.
[35] DE HERT P, GUTWIRTH S. Privacy, data protection and law enforcement: opacity of the individual and transparency of power[M]//CLAES E, DUFF A, GUTWIRTH S. Privacy & the criminal law. Oxford: Intersentia, 2006:61 -104.
[36] BLUME P. The citizens' data protection[EB/OL]. [2020 -08 -06]. https://warwick. ac. uk/fac/soc/law/elj/jilt/1998_1/blume/.
[37] WALTERS R, TRAKMAN L, ZELLER B. Data protection law: a comparative analysis of Asia-Pacific and European approaches[M]. Gateway East: Springer Nature Singapore Pte Ltd. ,2019: 15.
[38] DOVE E S. The EU General Data Protection Regulation: implications for international scientific research in the digital era[J]. Journal of law, medicine & ethics,2018,46(4): 1013 -1030.
[39] LEENES R. Do they know me? deconstructing identifiability[J]. University of Ottawa law and technology journal, 2007,4(1/2): 135 -161.
[40] EUROPEAN COMMISSION. Guidelines on open access to scientific publications and research data in horizon 2020(version 3.2)[EB/OL]. [2020 -08 -06]. https://ec. europa. eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en. pdf.
[41] MONDSCHEIN C F, MONDA C. The EU's General Data Protection Regulation (GDPR) in a research context[M]//KUBBEN P, DUMONTIER M, DEKKER A. Fundamentals of clinical data science. Cham: Springer Nature Switzerland AG,2019:55 -71.
[42] PURTOVA N. The law of everything: broad concept of personal data and overstretched scope of EU data protection law[J]. Law, innovation and technology,2018,10(1):40 -81.
[43] 申晓雨,吴雅涵. 从谷歌被罚看 GDPR 数据隐私保护[J]. 法人,

2019(4):98 - 100.

[44] RADBOUD UNIVERSITY. FAQ GDPR in research[EB/OL]. [2020 - 08 - 01]. https://www.ru.nl/rdm/gdpr-research/faq-gdpr-research/.

[45] What is a data subject? [EB/OL].[2020 - 08 - 06]. https://eugdprcompliant.com/what-is-data-subject/.

[46] 盛小平,吴红. 科学数据开放共享活动中不同利益相关者动力分析[J]. 图书情报工作,2019, 63(17):40 - 50.

[47] 中华人民共和国民法典[EB/OL].[2020 - 08 - 07]. http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml.

[48] 刁胜先,何琪. 论我国个人信息泄露的法律对策——兼与 GDPR 的比较分析[J]. 科技与法律, 2019(3):49 - 57.

[49] HERT P, PAPAKONSTANTINOU V. The data protection regime in China: in-depth analysis [R]. Brussels: European Union, 2015.

[50] KATULIC T, KATULIC A. GDPR and the reuse of personal data in scientific research[C]// SKALA K, KORICIC M, GRBAC T G, et al. 2018 41st international convention on information and communication technology, electronics and microelectronics (MIPRO). Rijeka: Croatian Society for Information and Communication Technology, Electronics and Microelectronics-MIPRO, c2018:1311 - 1316.

[51] 肖冬梅,谭礼格. 欧盟数据保护影响评估制度及其启示[J]. 中国图书馆学报,2018,44(5):76 - 86.

作者贡献说明：

盛小平:论文写作与修订;

杨绍彬:参与论文初稿写作。

Analysis on the Applicabilities and Functions of GDPR to Personal Data Protection in Open Sharing of Scientific Data

Sheng Xiaoping　Yang Shaobin

School of Library, Information and Archives, Shanghai University, Shanghai 200444

Abstract: [**Purpose/significance**] This paper provides reference for the protection of personal data in the process of open sharing of scientific data in China by analyzing the relevant provisions of the European Union's General Data Protection Law (GDPR). [**Method/process**] Using text analysis method, this paper reviewed the researches of GDPR and personal data protection, and analyzed the applicabilities of and the functions of GDPR to personal data protection in open sharing of scientific data and its enlightenments to China. [**Result/conclusion**] GDPR has many normative functions for the personal data protection in open sharing of scientific data, including defining the basic concepts of personal data protection and the scope of protection objects, the main principles, the main rights of the data subjects, the main responsibilities and obligations of the data controllers and processors, and laying the legitimacy foundation of personal data processing. GDPR's enlightenment to China is that we should establish and perfect the legal system of personal data protection in China, strengthen the risk management of personal data in open sharing of scientific data, and build a dynamic and traceable open sharing system of scientific data, so as to realize the protection of personal data in open sharing of scientific data in China.

Keywords: scientific data　open sharing　data protection　personal data　GDPR